PENGANTAR KEAMANAN SIBER

NAMA :VENI VIRDA HARIATI

NIM : 0220120003

PRODI ILMU KOMPUTER

FAKULTAS TEKNIK UNIVERSITAS ISLAM

AL – AZHAR MATARAM

Tugas :

1. **Mencari Link Web Yang Diinginkan**
   - Link unizar

   - Allintext unizar

- Intext unizar

- Allintitle unizar

- Intitle unizar

- Allinurl unizar

- Inurl unizar

2. **Hasil SS pencarian Web Unizar**
   1. **10 Des 2012**

2. 11 Januari 2013

3. 31 May 2013

4. 19 Agustus 2013

5. 16 May 2014

6. 18 December 2014

7. 28 Maret 2015

Magnificent Logo

- Home
- Yayasan
    - Yayasan Pesantren Luhur Al-Azhar
- Rektorat
    - Universitas Islam Al-Azhar
    - Kalender Akademik
- Fakultas
    - Fakultas Teknik
    - Fakultas Ekonomi
    - Fakultas Pertanian
    - Fakultas Hukum
    - Fakultas MIPA
    - Fakultas Kedokteran
- Lembaga
- Pendaftaran
    - Kontak
    - Download
- Dokumentasi
- Sitemap
- Webmail

ategories

- Berita
- Kemahasiswaan

rchives

- March 2015

andom Posts

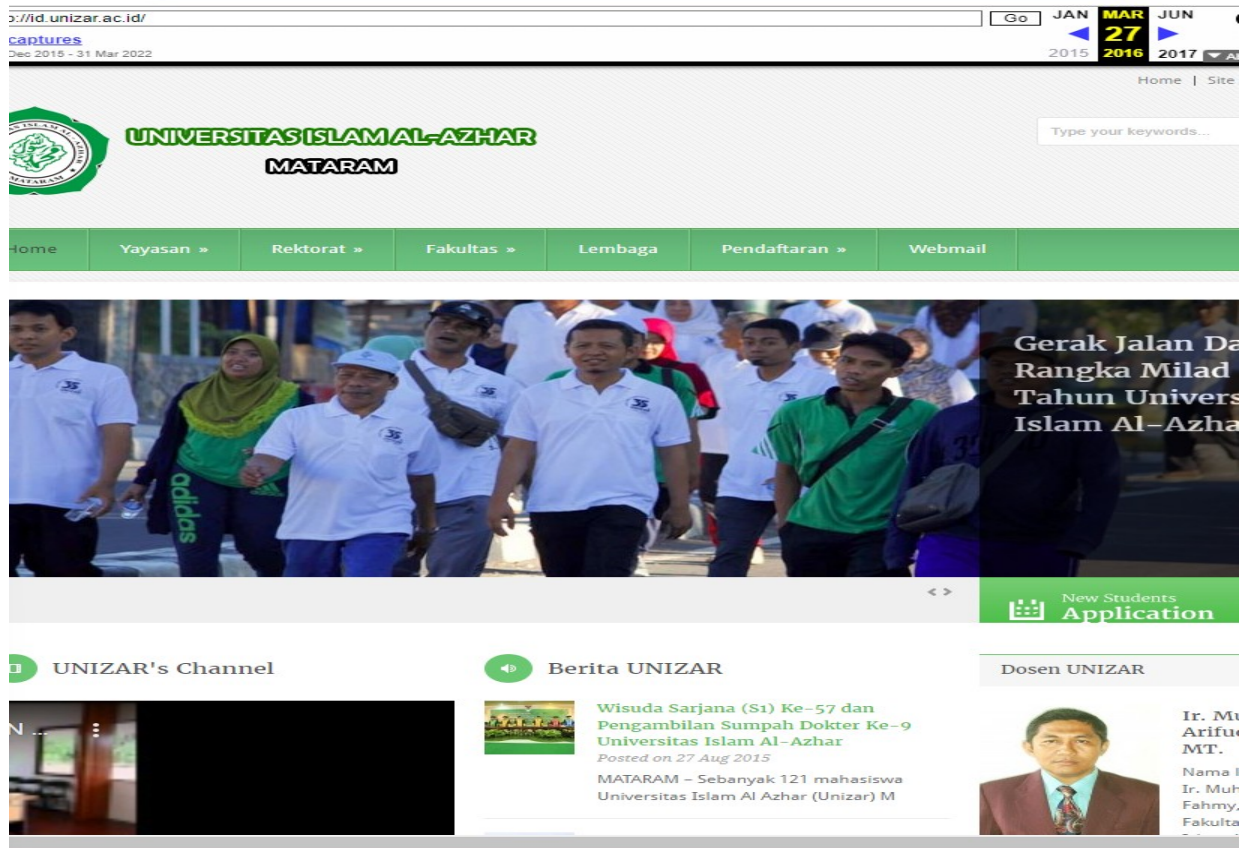
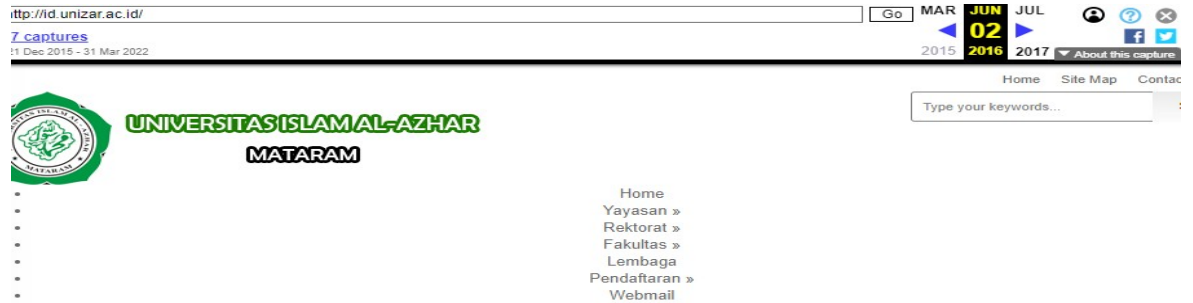
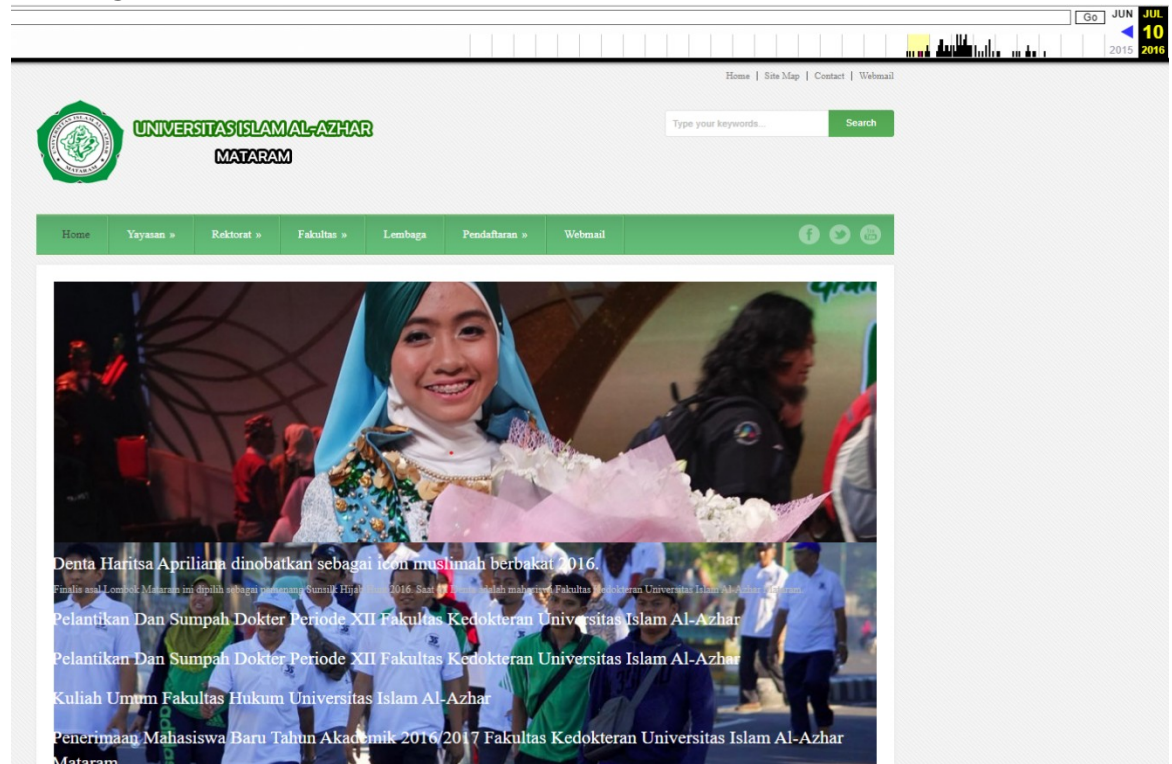
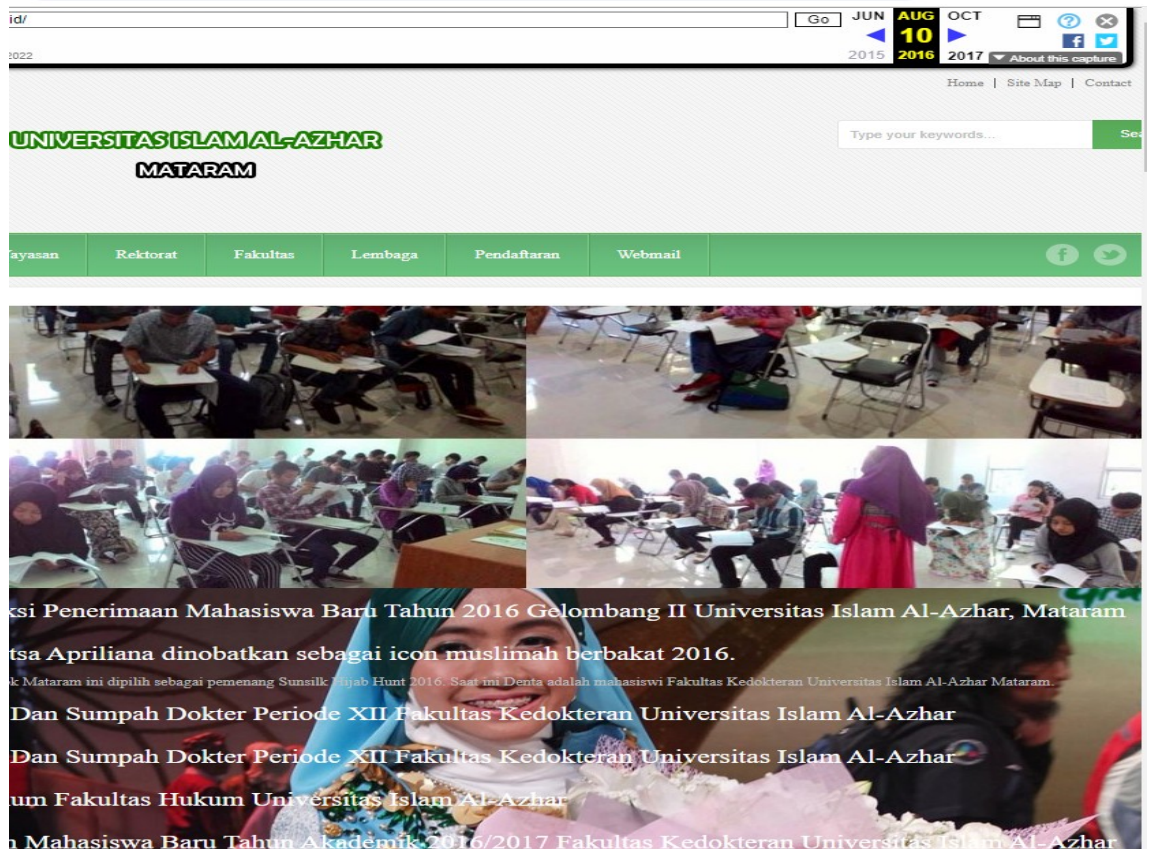
- Kebijakan Dan Strategi Dalam Pencegahan Dan Pemberantasan Penyalahgunaan Dan Peredaran Gelap Narkoba Kebijakan Dan Strategi Dalam Pencegahan Dan Pemberantasan Penyalahgunaan Dan Peredaran Gelap Narkoba

  Posted on Mar 19, 2015
- Mahasiswa Kedokteran Unizar Gelar KKL Kesmas Mahasiswa Kedokteran Unizar Gelar KKL Kesmas

  Posted on Mar 18, 2015
- Kesehatan Masyarakat Kesehatan Masyarakat

  Posted on Mar 19, 2015
- 240 Mahasiswa Unizar Ikuti Pembekalan KKN 240 Mahasiswa Unizar Ikuti Pembekalan KKN

8. 12 Januari 2016

9. 27 Maret 2016

10. 02 Juni 2016

11. 10 Juli 2016

12. 10 Agustus 2016

13. 15 Oktober 2016

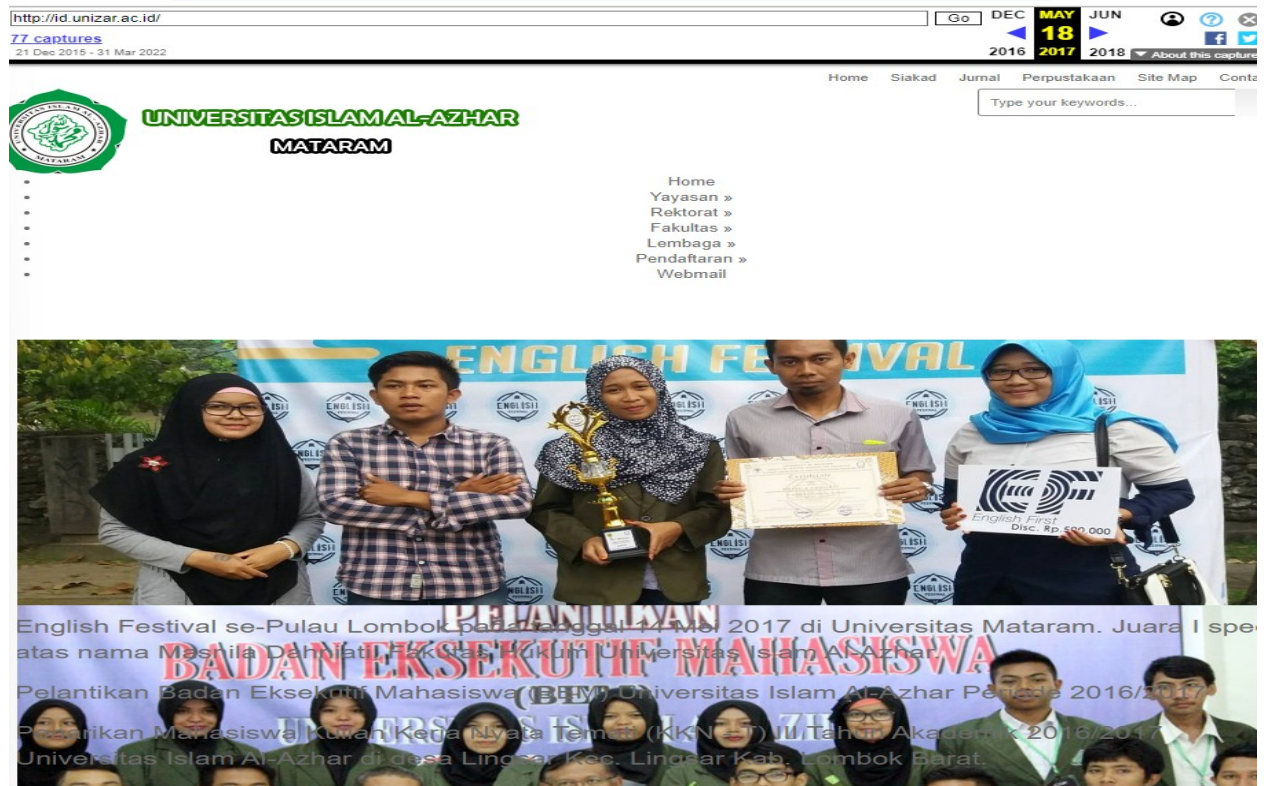
14. 11 November 2016

15. 16 November 2016

16. 1 December 2016

17. 29 April 2017

18. 09 May 2017

19. 18 May 2017

20. 18 Juni 2017

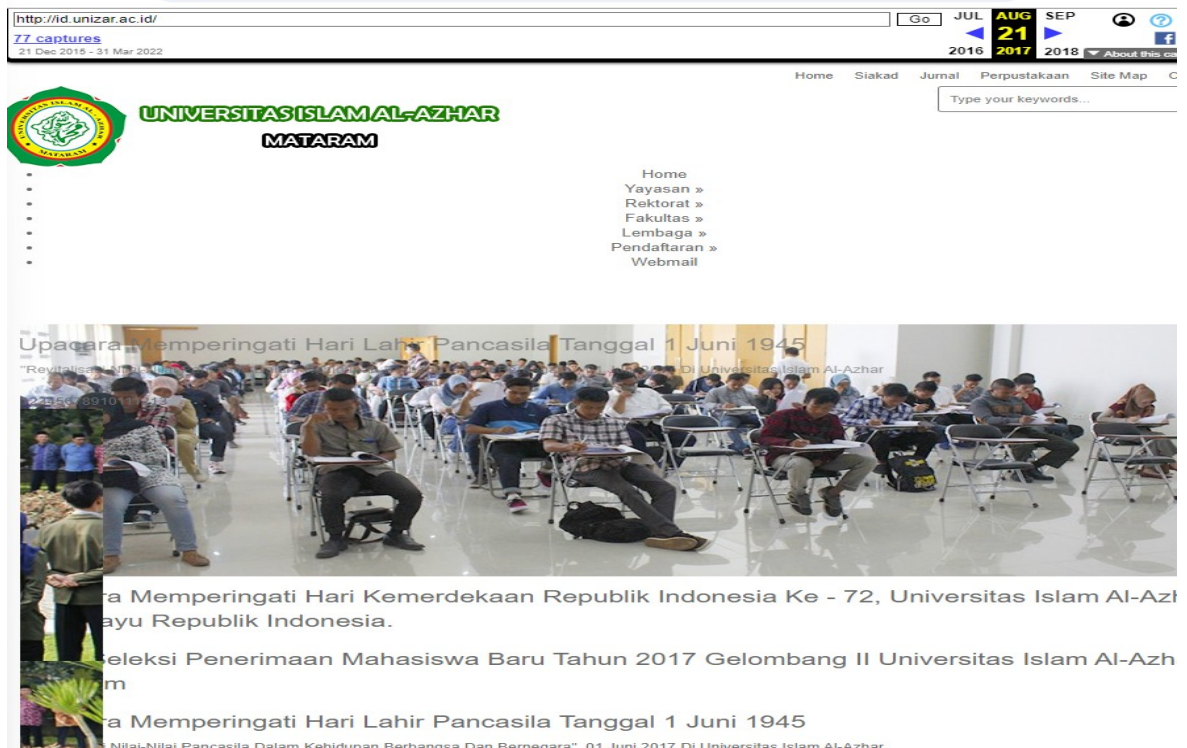
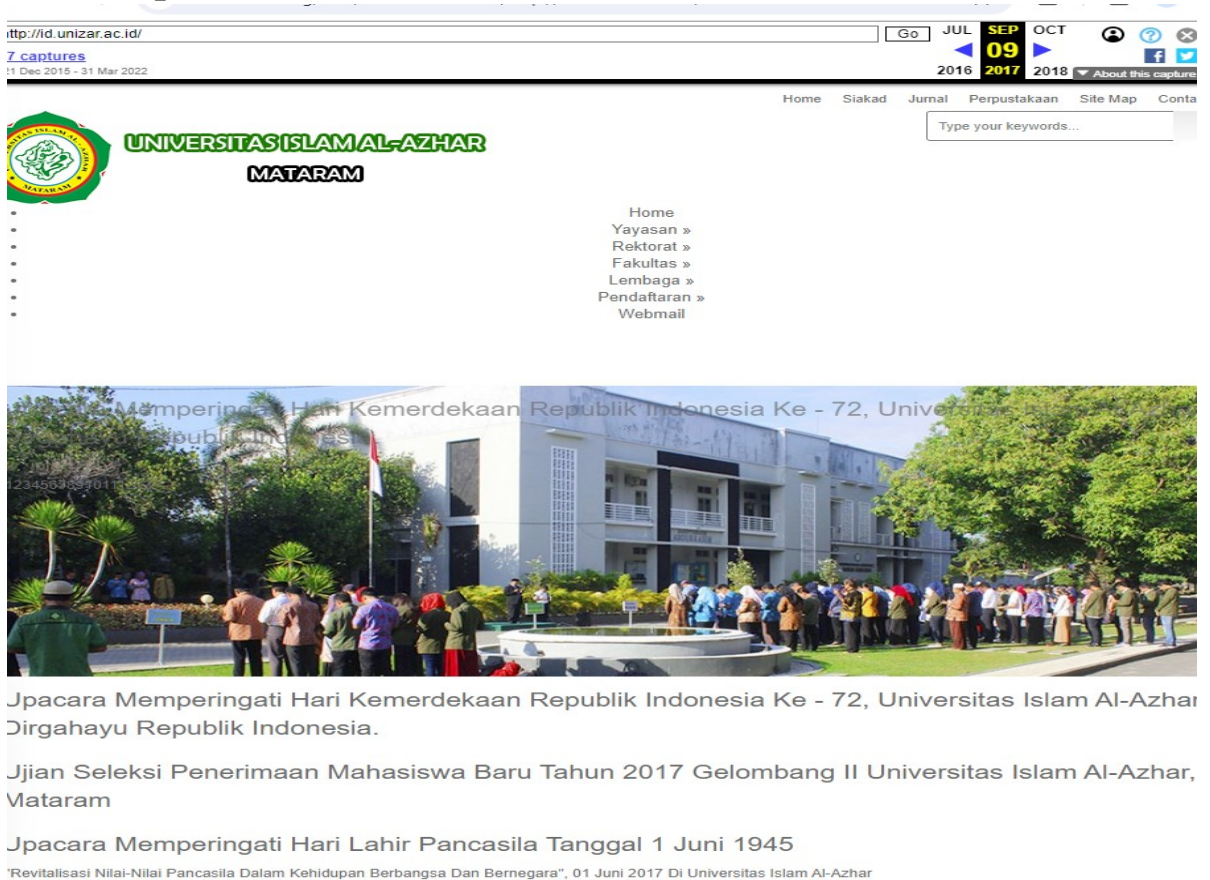
21. **26 Juni 2017**

22. **29 Juni 2017**

23. 29 Juni 2017

24. 19 Juli 2017

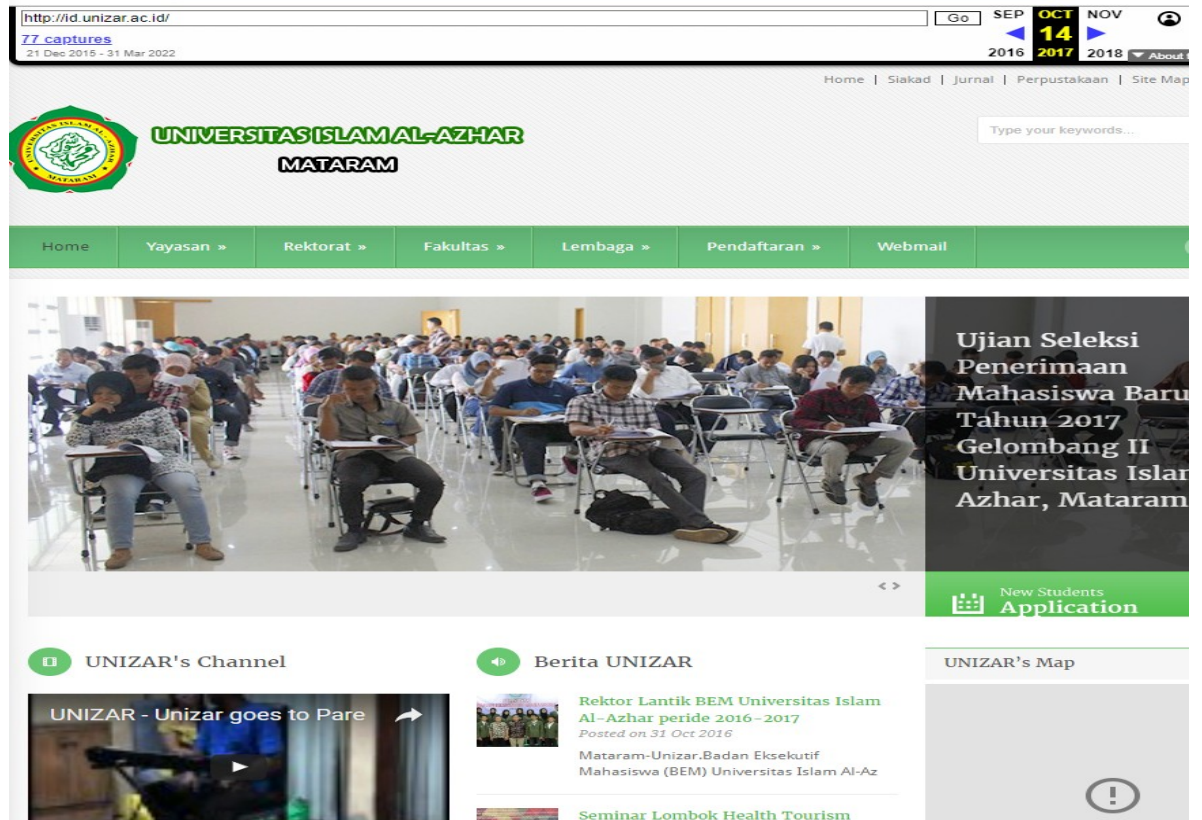
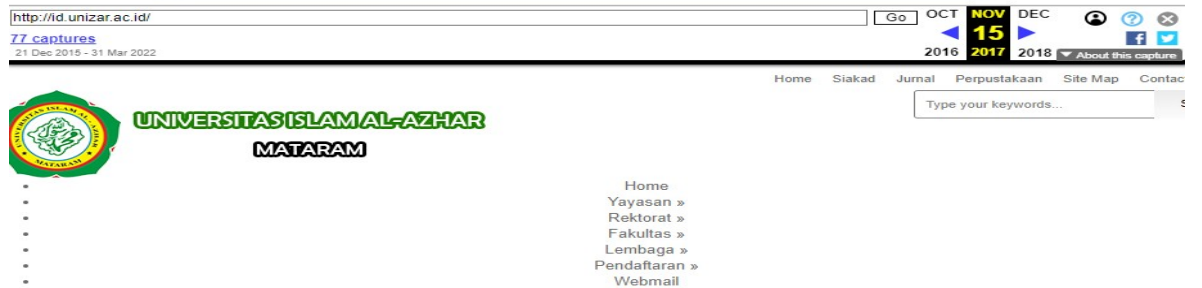
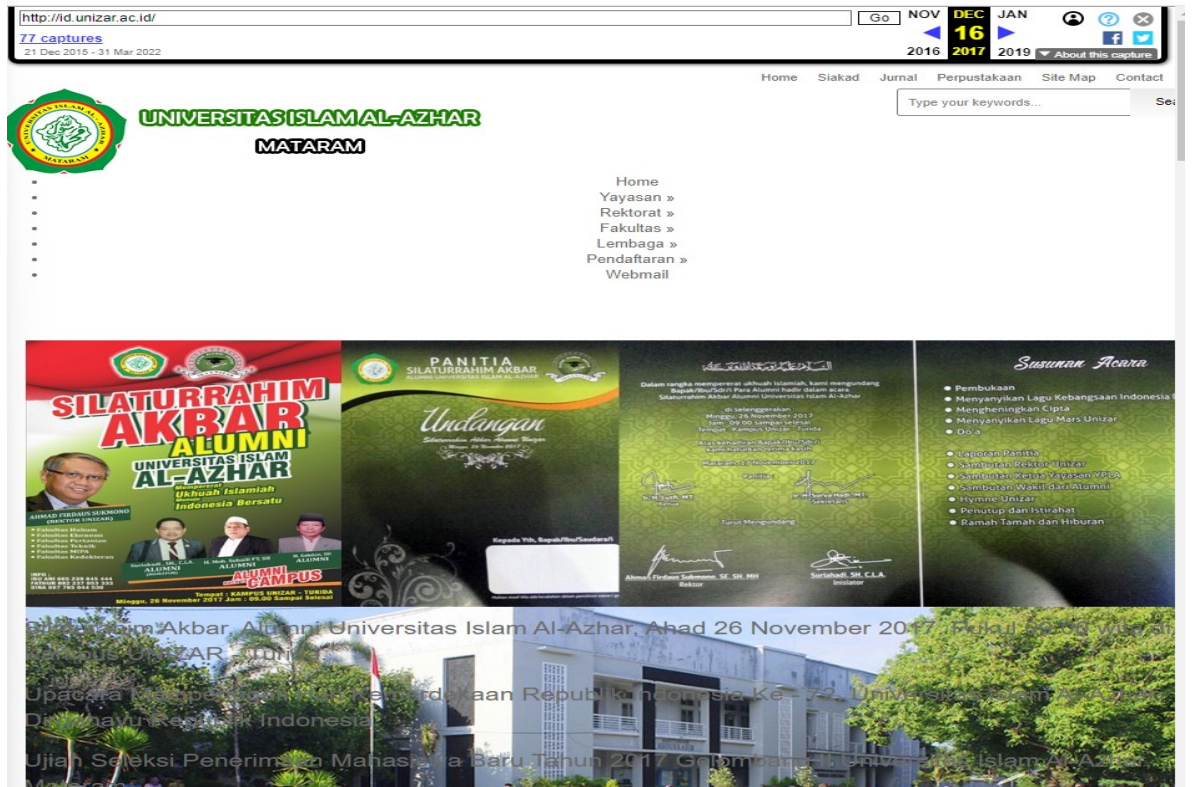
25. **21 Juli 2017**

26. **21 Agustus 2017**

27. 09 September 2017

Jpacara Memperingati Hari Kemerdekaan Republik Indonesia Ke - 72, Universitas Islam Al-Azhar
Dirgahayu Republik Indonesia.

Jjian Seleksi Penerimaan Mahasiswa Baru Tahun 2017 Gelombang II Universitas Islam Al-Azhar, Mataram

Jpacara Memperingati Hari Lahir Pancasila Tanggal 1 Juni 1945
'Revitalisasi Nilai-Nilai Pancasila Dalam Kehidupan Berbangsa Dan Bernegara", 01 Juni 2017 Di Universitas Islam Al-Azhar

28. 28 September 2017

29. 10 October 2017

30. 14 October 2017

33. 18 Desember 2017

34. 10 Januari 2018

35. 19 Januari 2018

36. 21 Februari 2018

37. 07 Marat 2018

38. 29 Maret 2018

39. 31 Maret 2018

40. 18 April 2018

41. 19 April 2018

42. 03 Mei 2018

43. 23 Mei 2018

44. 29 Mei 2018

45. 03 Juni 2018

46. 19 Juni 2018

47. 05 Juli 2018

48. 19 Juli 2018

49. 30 Juli 2018

50. 05 Agustus 2018

51. 07 Agustus 2018

52. 18 Agustus 2018

53. 29 Agustus 2018

54. 07 September 2018

55. 12 September 2018

56. 03 october 2018

57. 10 october 2018

58. 30 November 2018

59. 02 Janurai 2019

60. 14 Januari 2019

61. 16 Maret 2019

62. 16 Mei 2019

63. 23 Juli 2019

64. 29 Juli 2019

65. 11 September 2019

66. 11 Maret2020

67. 28 Januari 2021

Jniversitas Islam Al Azhar

Email : pustik@unizar.ac.id | Phone : (0370) 6175565

Facebook-f □
Twitter □
Youtube □
nstagram □

UNIVERSITAS ISLAM AL AZHAR

□

- Profil

Pendidikan

- Program Pendidikan
- Penerimaan Mahasiswa Baru
- Informasi Beasiswa

Fasilitas

- Sarana & Prasarana
- Teknologi Informasi (IT)
- Perpustakaan
- Fasilitas Lainnya

- LPPM
- BPM

68.02 Maret 2021

universitas islam al azhar

Pilihan Program Pendidikan

Temukan program pendidikan dan bidang studi yang sesuai dengan minat belajar Anda

Daftar Sekarang

Penerimaan Mahasiswa Baru

Sudah punya pilihan program pendidikan? Daftarkan diri Anda sekarang

Daftar Sekarang

Informasi Beasiswa

Informasi tentang berbagai skema beasiswa yang ditawarkan untuk mahasiswa baru

Daftar Sekarang

69.15 April 2021

universitas islam al azhar

Pilihan Program Pendidikan

Temukan program pendidikan dan bidang studi yang sesuai dengan minat belajar Anda

Daftar Sekarang

Penerimaan Mahasiswa Baru

Sudah punya pilihan program pendidikan? Daftarkan diri Anda sekarang

Daftar Sekarang

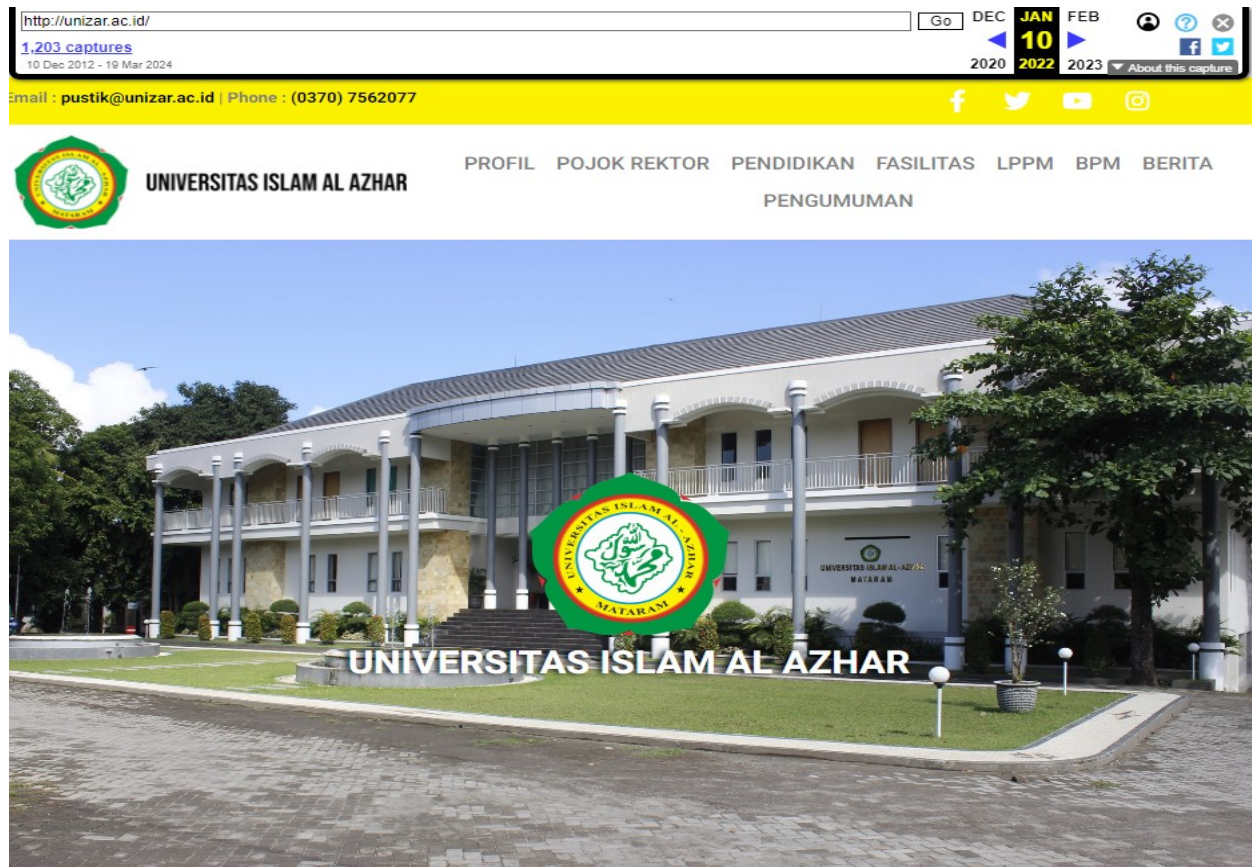
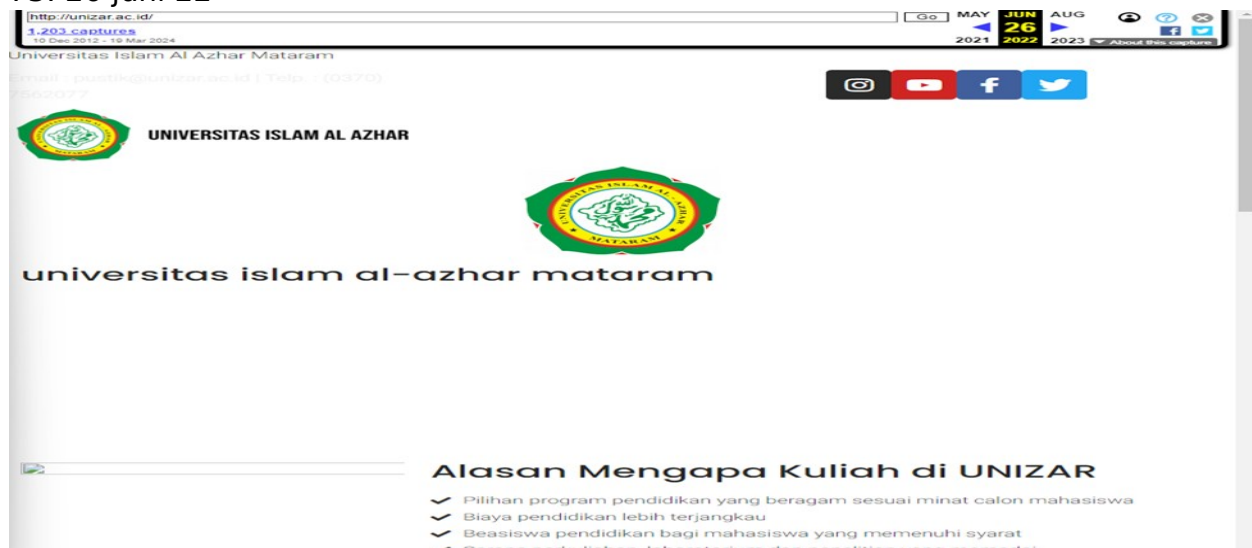
Informasi Beasiswa

Informasi tentang berbagai skema beasiswa yang ditawarkan untuk mahasiswa baru

Daftar Sekarang

70.07 Januari 2022

71.09 Januari 2022

72. 10 Januari 2022

73. 26 juni 22

74. 02 desmber 2022

http://www.unizar.ac.id/ Go NOV DEC JAN
1,203 captures 02
10 Dec 2012 - 19 Mar 2024 2021 2022 2023 About this capture

Ubuntu Logo

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`,

75. 03 desember 2022

http://www.unizar.ac.id/ Go NOV DEC JAN
1,203 captures 03
10 Dec 2012 - 19 Mar 2024 2021 2022 2023 About this capture

Ubuntu Logo

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf` . See their respective man pages for detailed information.

76. 04 desember 2022

http://www.unizar.ac.id/ Go NOV DEC JAN
1,203 captures 04
10 Dec 2012 - 19 Mar 2024 2021 2022 2023 About this capture

![Ubuntu Logo]

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`,

77. 05 desember 2022

http://www.unizar.ac.id/ Go NOV DEC JAN
1,203 captures 05
10 Dec 2012 - 19 Mar 2024 2021 2022 2023 About this capture

![Ubuntu Logo]

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf` . See their respective man pages for detailed information.

78. 06 desember2022

http://www.unizar.ac.id/ Go NOV DEC JAN
1,203 captures
10 Dec 2012 - 19 Mar 2024
2021 06 2022 2024 About this capture

Ubuntu Logo

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite,

79. 07 desember 2022

http://www.unizar.ac.id/ Go NOV DEC JAN
1,203 captures
10 Dec 2012 - 19 Mar 2024
2021 07 2022 2024 About this capture

Ubuntu Logo

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/

80. 08 desember 2022

http://www.unizar.ac.id/ Go NOV DEC JAN
1,203 captures 08
10 Dec 2012 - 19 Mar 2024 2021 2022 2024 About this capture

Ubuntu Logo

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite,

81. 09 desember 2022

http://www.unizar.ac.id/ Go NOV DEC JAN
1,203 captures 09
10 Dec 2012 - 19 Mar 2024 2021 2022 2024 About this capture

Ubuntu Logo

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.

82. 10 desember 2022

http://www.unizar.ac.id/

1,203 captures

10 Dec 2012 - 19 Mar 2024

NOV DEC JAN

2021 10 2022 2024

Ubuntu Logo

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`,

83. 11 desember 2022

http://www.unizar.ac.id/

1,203 captures

10 Dec 2012 - 19 Mar 2024

NOV DEC JAN

2021 11 2022 2024

Ubuntu Logo

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`,

84 .12 Desmber 2022

86.29 Mei 2023

87.06 Juni 2023

88.08 Juli 2023

89.24 September 2023

90.29 November 2023

Ubuntu Logo

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`,

91.19 Maret 2024

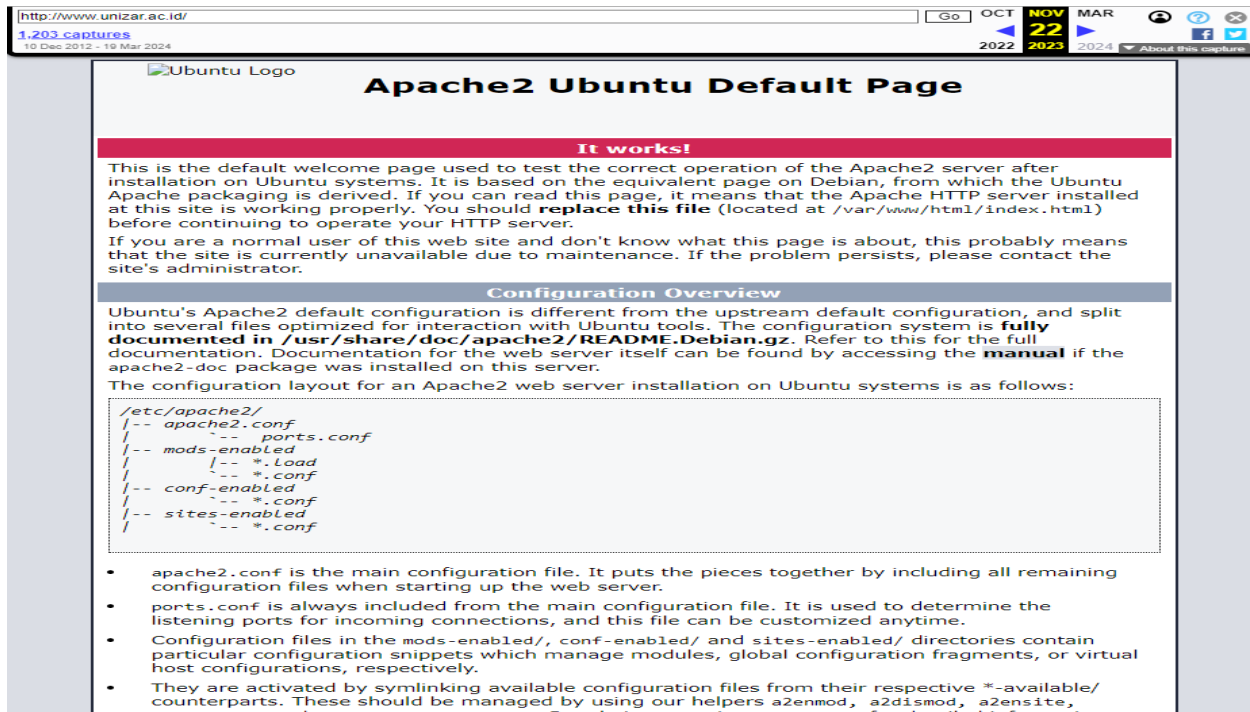
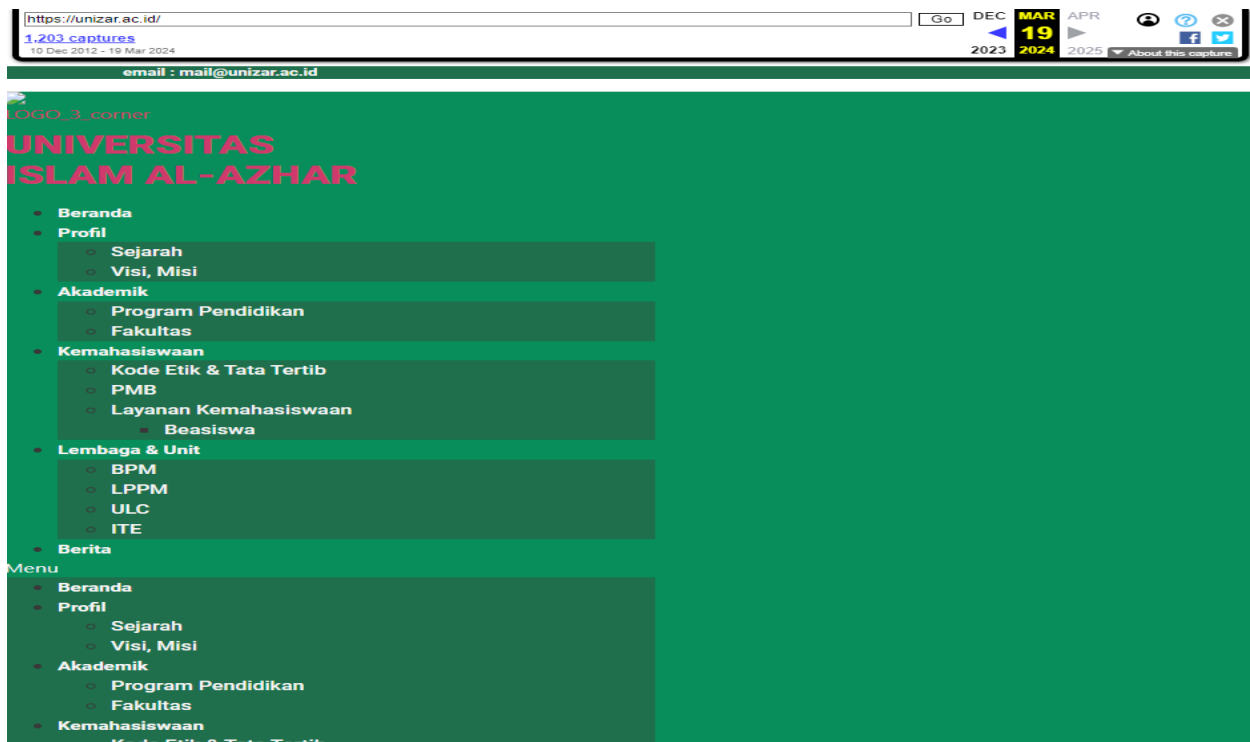
email : mail@unizar.ac.id

LOGO_3_corner

UNIVERSITAS
ISLAM AL-AZHAR

- Beranda
- Profil
  - Sejarah
  - Visi, Misi
- Akademik
  - Program Pendidikan
  - Fakultas
- Kemahasiswaan
  - Kode Etik & Tata Tertib
  - PMB
  - Layanan Kemahasiswaan
    - Beasiswa
- Lembaga & Unit
  - BPM
  - LPPM
  - ULC
  - ITE
- Berita

Menu

- Beranda
- Profil
  - Sejarah
  - Visi, Misi
- Akademik
  - Program Pendidikan
  - Fakultas
- Kemahasiswaan
  - Kode Etik & Tata Tertib

Tugas Praktik : Pengantar Keamanan Siber

Nama : Veni Virda Hariati

Nim :0220120003

Fakultas :Teknik

Prodi :Ilmu Komputer

UNIVERSITAS ISLAM AL-AZHAR

MATARAM

Social Engineering

Pengertian

Teknologi semakin canggih seiring perkembangan zaman, begitu pula dengan metode ancaman siber yang semakin beragam. Banyak penjahat siber yang memanfaatkan kecanggihan teknologi untuk mencuri data-data penting, privasi, bahkan harta berharga seperti uang. Salah satu serangan siber yang perlu Anda waspadai adalah social engineering.

Apakah Anda sudah tahu apa itu social engineering, bagaimana cara kerjanya, dan berbagai informasi terkait? Simak artikel berikut untuk mengetahui lebih lanjut.

Apa Yang Dimaksud Dengan Social Engineering

Rekayasa sosial atau biasa disebut social engineering adalah ancaman siber yang ditujukan bukan pada sistem komputer melainkan pada pengguna atau user, yaitu manusia. Seperti kebanyakan serangan siber, rekayasa sosial dilakukan untuk mengeksploitasi informasi pribadi, akses, atau harta berharga. Serangan ini bisa terjadi online maupun secara langsung. Setelah penyerang memahami apa yang memotivasi tindakan pengguna, mereka bisa menipu dan manipulasi pengguna.

Bagaimana Cara Kerja Rekayasa Sosial

Social engineering attack biasanya diawali dengan penyerang menganalisis korban terlebih dahulu. Jika targetnya adalah perusahaan, maka penyerang bisa mengumpulkan informasi terkait struktur organisasi, operasi internal, jargon perusahaan, ataupun mitra bisnis. Penyerang menargetkan pola perilaku karyawan yang memiliki akses terbatas seperti satpam atau resepsionis, dengan memindai profil media sosial untuk mendapatkan informasi pribadi dan mempelajari perilaku mereka baik online maupun offline. Setelahnya, penyerang dapat mempersiapkan serangan berdasarkan informasi yang sudah dikumpulkan dan mulai mengeksploitasi kerentanan yang ditemukan saat proses pengintaian. Jika serangan berhasil, penyerang memperoleh informasi rahasia seperti nomor.

Jenis-jenis Serangan Social Engineering

Phishing

Phising sering kali menggunakan email penipuan yang disamarkan sebagai email dari sumber terpercaya, tujuannya untuk menipu penerima email agar mengungkapkan informasi pribadi atau mengklik tautan yang dipasang malware.

Baiting

Penyerang meninggalkan perangkat fisik yang terinfeksi malware, seperti USB flash drive. Target kemudian mengambil perangkat dan memasukkannya ke komputer mereka, tanpa sengaja memasang malware.

Spear Phishing

Mirip dengan phishing, tetapi serangannya disesuaikan dengan orang atau organisasi tertentu.

Vishing

Biasa dikenal sebagai voice phising, dilakukan melalui telepon untuk memperoleh informasi keuangan atau pribadi dari target.

Whaling

Merupakan jenis serangan phishing yang menargetkan karyawan high-profile, seperti chief financial officer atau CEO, untuk mengelabui karyawan yang ditargetkan agar mengungkapkan informasi sensitif.

Dampak Buruk Social Engineering Pada Cybersecurity

Social engineering membawa berbagai damocial engineering memiliki teknik yang beragam tergantung pada media yang dipakai, beberapa diantaranya yang lazim ditemukan meliputi disebabkan oleh rekayasa sosial pada cybersecurity diantaranya:

Diserang Ransomware

Dampak rekayasa sosial terhadap bisnis seringkali disebabkan oleh malware, yang dirancang dengan tujuan untuk menginfeksi, mengenkripsi, dan menyandera file untuk tebusan. Perusahaan harus membayar biaya yang tidak kecil untuk memulihkan aset dan data yang disandera, atau hal-hal penting tersebut akan hilang selamanya. Konsekuensinya, perusahaan bisa kehilangan kepercayaan publik dan klien.

Menjadi Mangsa Watering Hole Attack

Watering hole attack menggunakan situs web perusahaan yang sering dikunjungi sebagai tempat berkembang biaknya infeksi virus. Kerusakannya tidak hanya mempengaruhi perusahaan saja, tetapi juga pelanggan maupun

calon pelanggan. Meskipun serangan ini terkenal sulit dicegah, tetaplah selalu perbaharui keamanan sistem Anda.

Kehilangan Data

Peretas terkadang mencuri data-data penting dan kemudian menjualnya di dark web untuk mendapatkan keuntungan besar, selain itu hal ini juga dilakukan untuk mempermalukan atau mengekspos perusahaan.

Contoh Kasus Serangan Social Engineering di Indonesia

Teknologi yang semakin canggih menyebabkan maraknya kasus social engineering attack sering terjadi di Indonesia, beberapa diantaranya adalah:

Penipuan Dengan Mengeksploitasi Data Pribadi di Instagram

Pada tahun 2021, Instagram sempat mengeluarkan fitur Add Yours yang memungkinkan pengguna memberikan opini, informasi, hingga bahkan informasi pribadi berdasarkan topik tertentu. Data pribadi yang terkumpul pada fitur ini menjadi celah penipuan melalui telepon dimana seseorang akan mengaku sebagai kerabat dekat dan meminta bantuan berupa uang. Korban yang langsung percaya setelah mengobrol akrab selama beberapa waktu kemudian mengirimkan uang hingga jutaan rupiah dengan asumsi hal tersebut akan membantu kerabatnya.

Serangan Email Phishing Melanda Pelaku UMKM

Banyak pelaku bisnis UMKM di Indonesia menjadi korban serangan phishing yang dilakukan oleh penjahat siber semenjak pandemi terjadi. Data dari perusahaan keamanan Kaspersky mencatat, terdapat 192.591 serangan phising yang terjadi pada bisnis UMKM di Indonesia selama kuartal pertama 2020. Penyerang mengirimkan email berisikan informasi terkait COVID-19 untuk memancang rasa keingintahuan dan kepanikan dari korban.

Penipuan Menggunakan Aplikasi Mobile Banking Palsu

Belakangan ini, nasabah bank dihimbau agar berhati-hati terhadap penipuan yang menggunakan aplikasi mobile banking palsu. Dalam aksinya, penipu mengirimkan pesaan secara acak melalui Whatsapp dan mengelabui korban untuk memasukkan informasi akun pada aplikasi palsu tersebut. Setelah berhasil mendapatkan data sensitifini, penipu akan langsung mengambil alih akun milik korban dan melakukan transfer uang ke rekening yang telah disiapkan.

Tips Untuk Mengatasi Terjadinya Rekayasa Sosial

Meskipun metode penipuan social engineering semakin beragam, ada beberapa tips yang bisa dilakukan untuk menghindarinya yaitu:

Otentikasi Multi Faktor

Ini merupakan tindakan pencegahan paling dasar untuk melindungi keamanan akun anda. Karena rekayasa sosial dapat digunakan untuk mendapatkan akses ke kata sandi, otentikasi multifaktor yang mencakup akses biometrik, pertanyaan keamanan, maupun kode OTP sangatlah penting diimplementasikan.

Memantau Celah Dengan Pemikiran Kritis

Kembangkan pemikiran kritis dalam mengantisipasi tanda-tanda serangan social engineering terutama pada sistem atua perangkat yang menyimpan informasi sensitif. Selalu pantau sistem secara berkala dan lakukan pemindaian kerentanan dalam sistem baik itu berasal dari eksternal maupun internal.

Perhatikan Jejak Digital

Berbagi data pribadi secara berlebihan di media sosial dapat memberi para penyerang informasi lebih untuk dieksploitasi. Misalnya, jika Anda menyimpan resume Anda secara online, pastikan menghapus tanggal lahir, nomor telepon, dan alamat rumah. Semua informasi itu sering dimanfaatkan penyerang dalam melancarkan social engineering.

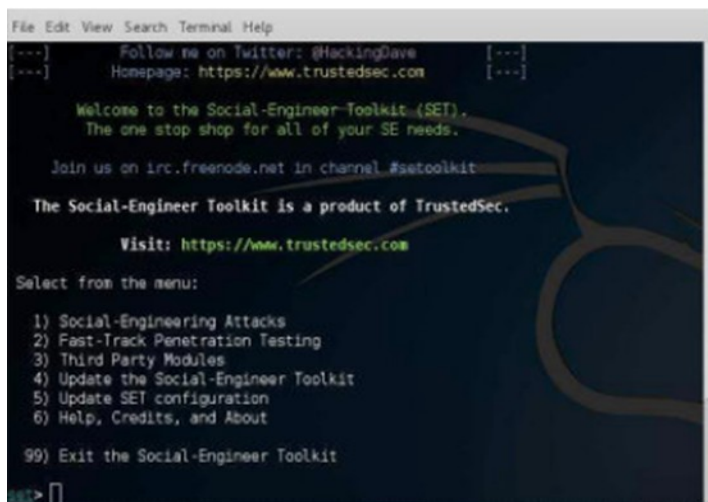
Menggunakan Solusi Threat Intelligence Dari Aplikas

Aplikas Servis Pesona merupakan member dari Phintraco Group yang menyediakan solusi keamanan IT yang berkelas. Salah satu solusi yang disediakan Aplikas adalah threat intelligence yang menangani serangan dunia maya dengan mengidentifikasi motif, target, dan perilaku penjahat dunia maya dalam rangka menjaga nama baik perusahaan

Social Engineering atau dalam bahasa indonesianya Rekayasa Sosial merupakan suatu aksi kejahatan didunia maya dan menjadi ancaman terbesar pada zaman sekarang. Social Engineering sendiri menjadi sesuatu hal yang trending pada era perkembangan teknologi informasi saat ini, karena seiring dengan banyaknya perkembangan media social yang menyediakan fasilitas untuk bertukar informasi antara pengguna satu dengan pengguna yang lain, disisi lain hal ini menjadi peluang dan dimanfaatkan oleh orang-orang yang tidak bertanggung jawab untuk melakukan penipuan guna memperoleh keuntungan tersendiri dalam setiap aksinya. Social Engineering pertama kali di perkenal oleh seorang Hacker bernama Kevin Mitnik, dimana ia melakukan aksi hacking dan penipuan terhadap puluhan perusahan termasuk system keamanan negara,

perbankan, dan layanan komunikasi, Kevin Mitnik sendiri tertangkap pada tahun 1995 dan dijatuhi hukuman penjara dan denda ganti rugi senilai Rp.41.000.000,00 dan akhirnya ia dibebaskan pada tahun 2000.

Memperlihatkan dan memberitahukan kepada masyarakat umum, khususnya bagi mereka yang sering mengunakaan media social dalam kehidupan sehari-hari guna memperoleh informasi dan menjalin komunikasi dengan sahabat dan juga kerabat mereka, tentang bahaya dari teknik hacking dengan menggunakan metode social engineering pada media social, khususnya Facebook dan Twitter sebagai media media social yang paling popular pada saat ini. Dan tujuan dari penulisan jurnal ini agar memperlihatkan bagaimana cara kita browsing dengan aman didunia maya.

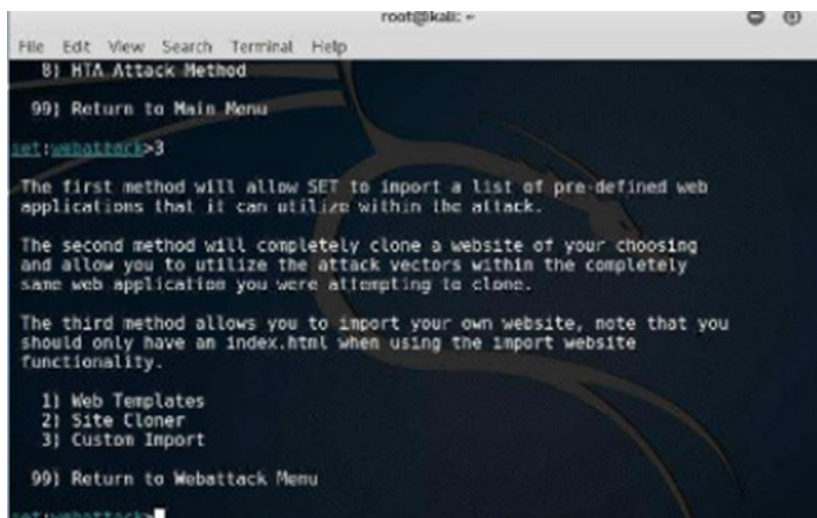
Langkah-Langkahnya

Phishing Phishing merupakan metode penipuan yang dilakukan dengan menggunakan media komunikasi berupa pesan text(SMS), telepon, e--mail dan juga website, untuk memperoleh informasi berupa, informasi akun, password, dan rekening bank milik korban. ⬧ Fake Login Fake login adalah teknik merekayasa tampilan login yang memiliki kesamaan seperti tampilan pada web login aslinya agar korban tertipu dan tidak mencurigai. ⬧ Exploitation OS Exploitation Os adalah aksi dimana attacker melakukan eksplorasi didalam system operasi korban, setelah attacker berhasil memasukan atau berhasil menginfeksi computer atau laptop korban dengan malware (malicious software) yang telah disispkan backdoor didalamnya. ⬧ Undectectable Backdoor Undectectable Backdoor adalah sebuah teknik dimana seorang attacker menyisipkan backdoor didalam sebuah software yang tidak bisa dideteksi oleh antivirus.

Pengumpulan data melalui buku, maupun internet sebagai landasan penelitian mengenai Social Engineering. ⬧ Penggunaan Sistem Operasi Kali Linux 2.2 (codename rolling) sebagai media simulasi pembuatan Sosial

Enginering. ⬩ Melakukan simulasi phishing melalui jaringan local maupun jaringan public, dengan memanfaatkan media social. ⬩ Melakukan simulasi pemaketan undectectable backdoor. ⬩ Melakukan simulasi exploitation operation system khusunya system operasi Microsoft windows sebagai target penyerangan. ⬩ Melakukan simulasi cloning template web login, baik web login social media, maupun web login pada website lainnya,sebagai metode fake login.

Pada tahapan ini akan dibahas tentang bagimana simulasi pembuatan paket-paket hacking yang bertujuan agar menyukseskan aksi social engineering yang akan kita buat serta metode-metode hacking lainnya yang sudah dijelaskan pada bagian sebelumnya. Tujuan dari pembahasan ini yang nantinya akan memperlihatkan langkah-langkah pembuatan paket-paket hacking serta teknik hacking berdasarkan metode social engineering terkini 2016.

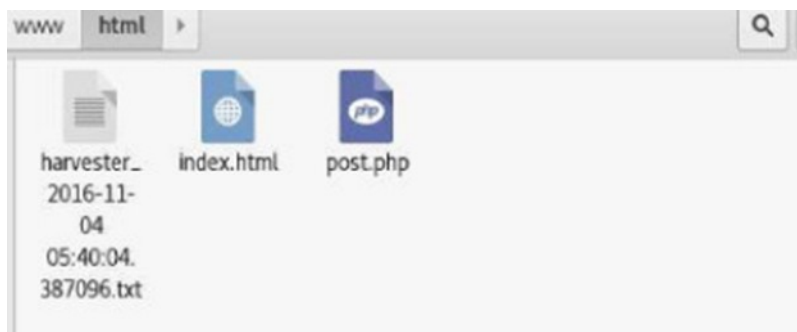
SET pada sistem operasi kali linux sejatinya dijalankan pada console atau terminal seperti kebanyakan tool-tool hacking lainnya di linux. Dan seperti pada gambar diatas SET menyediakan pilihan- pilihan hacking yang bisa dipilih

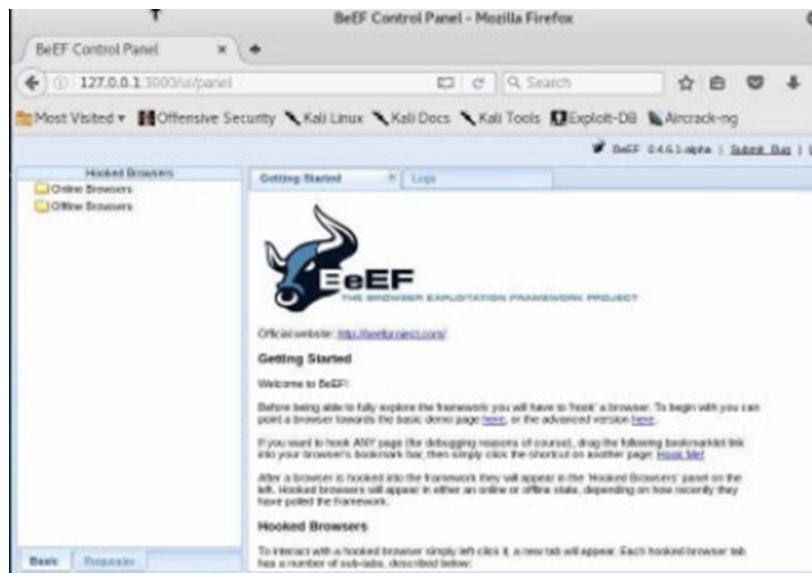
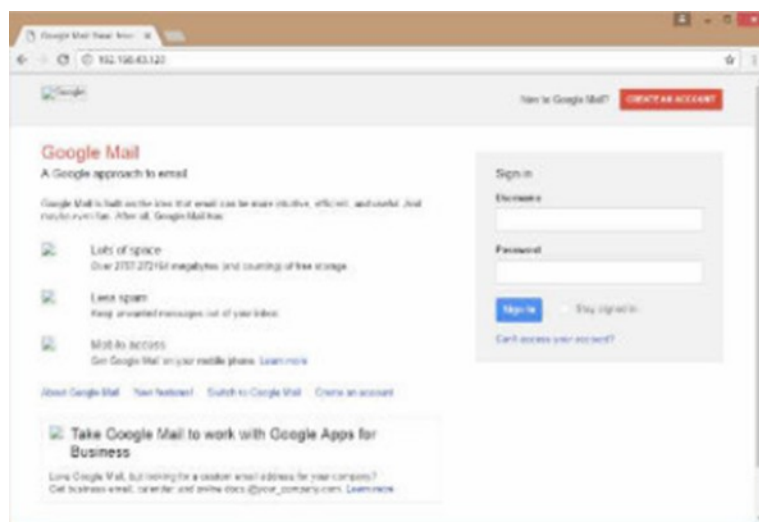
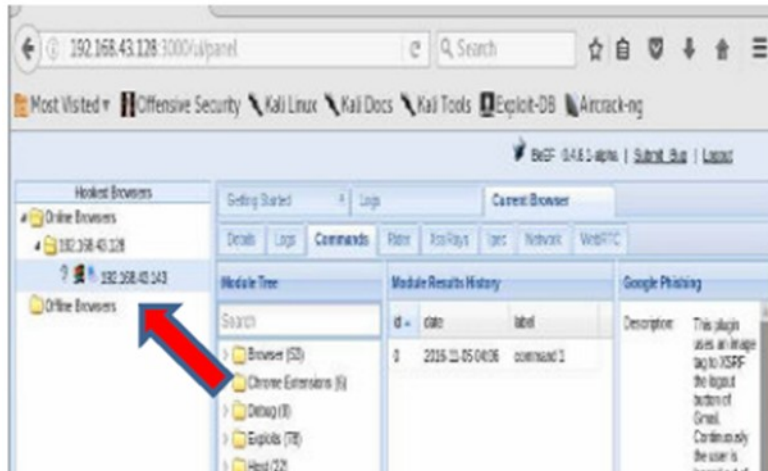
Ghost Phisher merupakan tools pada Kali Linux updetan terbaru yang menyediakan banyak fitur-fitur yang bersifat network dan vurnerable pentesting.

Tools yang digunakan untuk pembuatan teknik atau metode fake login yaitu menggabungkan dua tools yang sering digunakan oleh para attacker yaitu SET dan Beef-XSS-Framework. Pada metode kali ini SET berfungsi sebagai tools untuk cloning template web login sedangkan Beef-XSS- Framework berfungsi sebagai listener atau menerima korban yang sudah terjebak dari web login yang telah dibuat.

```
[-] to harvest credentials or parameters from a website as well as place them
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.

  1. Java Required
  2. Google
  3. Facebook
  4. Twitter
  5. Yahoo

set:webattack> Select a template:
```

Pada tahapan ini attacker menentukan pilihan untuk memilih media social mana saja yang akan digunakan untuk metode fake login. Pada gambar diatas tampak media social seperti Facebook dan Twitter tidak luput dari incaran attacker untuk memanipulasi Fake Web Login Template

memperlihatkan file index.html dari salah satu template web login social media yang sudah dicloning

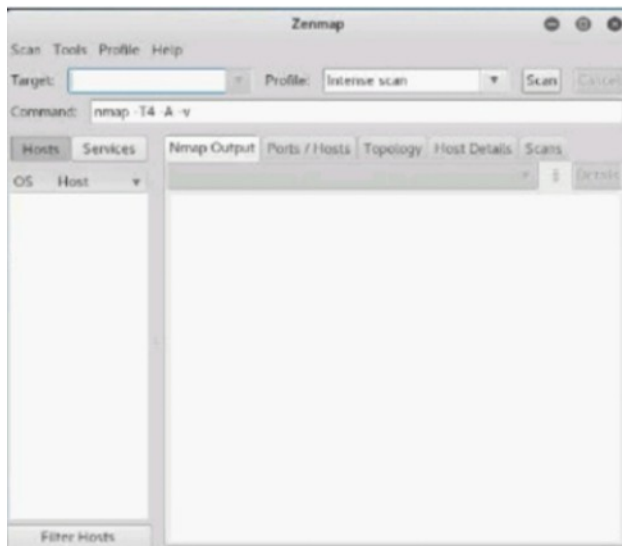
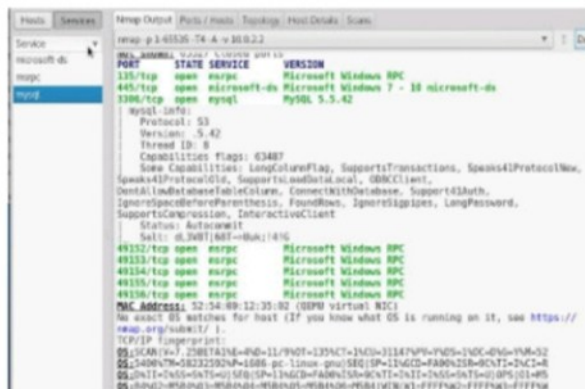
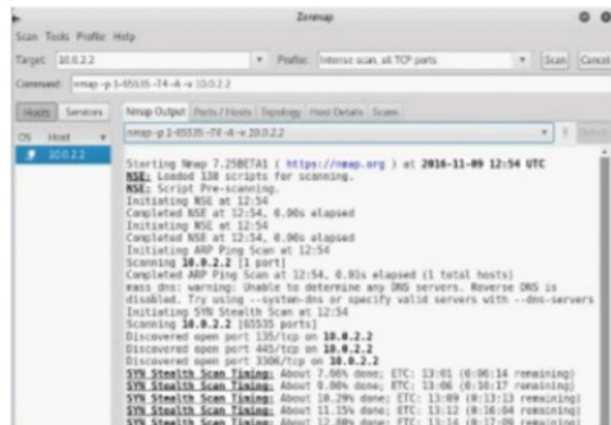
```
root@kali: /usr/share/beef-xss
File  Edit  View  Search  Terminal  Help
beef-xss: /usr/bin/beef-xss /etc/beef-xss /usr/share/beef-xss
root@kali:~# cd /usr/share/beef-xss
root@kali:/usr/share/beef-xss# ./beef
[ 3:57:15][*] Bind socket [imapeudoral] listening on [0.0.0.0:2000].
[ 3:57:15][*] Browser Exploitation Framework (BeEF) 0.4.6.1-alpha
[ 3:57:15]    |   Twit: @beefproject
[ 3:57:15]    |   Site: http://beefproject.com
[ 3:57:15]    |   Blog: http://blog.beefproject.com
[ 3:57:15]    |_  Wiki: https://github.com/beefproject/beef/wiki
[ 3:57:15][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[ 3:57:16][*] BeEF is loading. Wait a few seconds...
[ 3:57:25][*] 12 extensions enabled.
[ 3:57:25][*] 254 modules enabled.
[ 3:57:25][*] 2 network interfaces were detected.
[ 3:57:25][+] running on network interface: 127.0.0.1
[ 3:57:25]    |   Hook URL: http://127.0.0.1:3000/hook.js
[ 3:57:25]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[ 3:57:25][+] running on network interface: 192.168.43.128
[ 3:57:25]    |   Hook URL: http://192.168      :3000/hook.js
[ 3:57:25]    |_  UI URL:   http://192.168      3000/ui/panel
[ 3:57:25][*] RESTful API key: 8899fe250743b181a847a16d6b98ed899b0e126a
[ 3:57:25][*] HTTP Proxy: http://127.0.0.1:6789
[ 3:57:25][*] BeEF server started (press control-c to stop)
```

memperlihatkan tampilan Beef-xss-framework pada mozila firefox, beef-xss-framwork adalah tools pentesting yang dibangun menggunakan bahasa pemograman HTML (Hyper Text Markup Language) yang memiliki banyak fitur atau tools- tools hacking didalamnya

Pada simulasi kali ini, korban yang di phishing menggunakan system operasi Windows 8 dan brower internet korban yang telah di infeksi javascript pada beef- xss-framework ialah browser Google Crome seperti yang telah terlihat

memperlihatkan bagaimana attacker menerima pemberitahuan pada Beef Control Panel pada mozila firefox bahwa korban dengan IP Address 192.168.43.128 pada system operasi windows telah diterinfeksi javascript pada browser korban. Beef-Xss-Framework memiliki fitur-fitur hacking seperti Social Engineering, Exploit, Metasploit, Deface, Phishing dan lain-lain. Beef juga dapat menginfeksi browser pada

mobile phone dan semua jenis system operasi yang memiliki kelemahan pada browser.

Nmap

Network Mapper atau yang sering dikenal Nmap merupakan tools yang sering digunakan di unutk melakukan scanning terhadap service-service pada port yang terbuka (open) untuk mencari dan mengumpulkan informasi dari port-port tersebut.Port yang terrbuka melingkupi system operasi, jaringan dan lanyanan system seperti server dan lain-lain

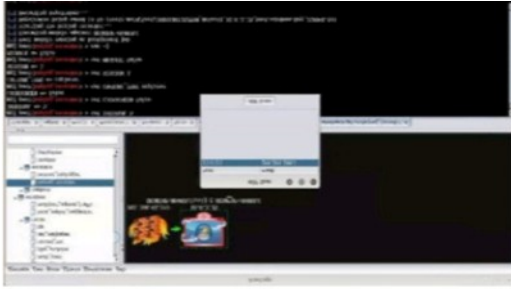
```
root@kali:~# nmap
Nmap 7.25BETA1 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
```

Tampilan Umum Nmap pada terminal kali Linux

Tampilan Zenmap Pada kali Linux

Pada gambar diatas mode scanning yang dilakukan secara intensif terhadap TCP (Transmission Control Protocol) Port pada system operasi windows 8 dan menampilkan service yang mengunakan port-port yang terbuka.

✓	135	tcp	open	msrpc	Microsoft Windows RPC
✓	445	tcp	open	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds
✓	3306	tcp	open	mysql	MySQL 5.5.42
✓	49152	tcp	open	msrpc	Microsoft Windows RPC
✓	49153	tcp	open	msrpc	Microsoft Windows RPC
✓	49154	tcp	open	msrpc	Microsoft Windows RPC
✓	49155	tcp	open	msrpc	Microsoft Windows RPC
✓	49156	tcp	open	msrpc	Microsoft Windows RPC

Armitage
Armitage merupakan tools berbasis GUI yang dibuat menggunakan bahasa pemograman Java dan memiliki fungsi untuk exploitasi pada system operasi. Armitage sejati sama seperti metasploit-framework namun memiliki perbedaan pada tampilannya

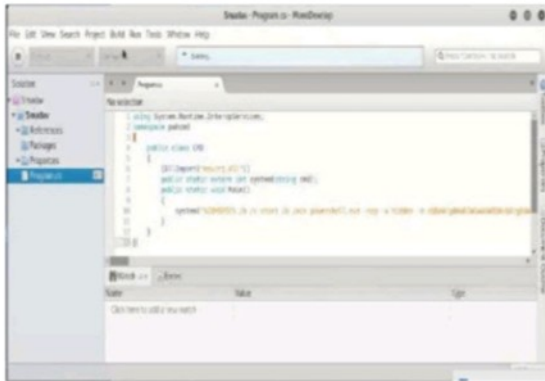
Tampilan Armitage

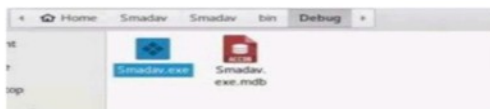
Pada simulasi seperti yang terlihat pada gambar diatas dimana system operasi yang menjadi target adalah windows 10 dengan alamat IP Addressnya 192.168.43.143 dan 10.0.2.15 merupakan IP Address Virtual MachineMachine

Memasang keyloger pada windows

menunjukan bagaimana teknik
memasang keyloger pada windows 10 dengan
menggunakan armitage.
Fungsi dari keyloger sendiri untuk merekam aktifitas
keyboard korban ketika melakukan surfing dan browsing
didunia maya.

Undetected Backdoor
Undetected backdoor merupakan program atau software
yang tidak bias terdeteksi baik antivirus maupun windows
defender. Dalam klasifikasinya undetected backdoor
sendiri tergolong dalam Malware (Malicious Software)
atau program jahat.

Tampilan pembuatan undetected Backdoor

diatas memperlihatkan cara pembuatan
undetected backdoor dengan menggunakan msfvenom pada
Kali Linux. Msfvenom adalah tools keluaran Metasploit
Framework yang bertujuan sebagai tools untuk membuat
paket-paket payload, exploit auxiliary dan lain-lain

Tampilan Monodevelopment pada Kali Linux.

menampilkan proses compile dengan
menggunakan monodevelopment pada Kali Linux. Monodevelopment merupakan aplikasi yang bersifat open source yang memiliki fungsi selayaknya Microsoft Visual Studio pada Microsoft Windows, monodevelopment mendukung bahasa pemograman seperti C, C++, C#, Asp.Net, VBnet dan lain-lain.

Hasil output compile pada folder.

Pada gambar diatas memperlihatkan hasil compile dalam bentuk file executable dengan nama Smadav.exe. Dalam simulasi kali ini undetected backdoor yang dibuat menggunakan bahasa pemograman C# dan berkarakter powershell-cmd.

Tampilan pada windows 10 ketika Smadav.exe
di jalankan.

Tampilan Power Shell pada windows 10 ketika

Aplikasi Smadav.exe yang berisi backdoor dieksekusi. menampilkan proses dimana aplikasi Smadav.exe di jalankan pada windows 10. Gambar 20 menampilkan pemberitahuan dari windows SmartScreen kepada user, apakah user bersedia dan mengiijinkan agar aplikasi Smadav.exe dapat dijalankan. Dan ketika user meng-klik tombol run maka Aplikasi Smadav.exe tersebut langsung berjalan dan menampilakn windows Power Shell seperti yang ditampilkan pada gambar 21 dan ketika aplikasi Smadav.

icon AdBlock Plugin.

Adblock adalah ekstensi peramban internet yang memblokir dan mencegah munculnya iklan pada situs web

icon noScript Plugin.

Xss merupakan salah satu jenis serangan injeksi code.Xss dilakukan oleh penyerang dengan cara memasukan kode HTML atau client script code lainnya ke suatu situs.